Secure Mobile Social Networks using USIM in a Closed Environment

Omer Nawaz
School of Computing
Blekinge Institute of Technology
Karlskrona, Sweden
Email: onz@bth.se

Christian Gehrmann
Secure Systems Group
Swedish Institute of Computer Science (SICS)
Kista, Sweden
Email: chrisg@sics.se

Markus Fiedler
School of Computing
Blekinge Institute of Technology
Karlskrona, Sweden
Email: markus.fiedler@bth.se

***Abstract*—Online social networking and corresponding mobile based applications are gaining popularity and now considered a well-integrated service within mobile devices. Basic security mechanisms normally based on passwords for the authentication of social-network users are widely deployed and poses a threat for the user security. In particular, for dedicated social groups with high confidentiality and privacy demands, stronger and user friendly principles for the authentication and identification of group members are needed. On the other hand, most of the mobile units already provide strong authentication procedures through the USIM/ISIM module. This paper explores how to build an architectural framework for secure enrolment and identification of group members in dedicated closed social groups using the USIM/SIM authentication and in particular, the 3GPP Generic Authentication Architecture (GAA), which is built upon the USIM/SIM capabilities. One part of the research is to identify the marketable use-cases with corresponding security challenges to fulfil the requirements that extend beyond the online connectivity. This paper proposes a secure identification design to satisfy the security dimensions for both online and offline peers. We have also implemented an initial proof of the concept prototype to simulate the secure identification procedure based on the proposed design. Our implementation has demonstrated the flexibility of the solution to be applied independently for applications requiring secure identification.**

***Keywords*—Mobile Social Networks, Information Security, Secure Identification.**

[1]

I. Introduction

Online social networking like Facebook and Twitter has brought revolution towards social life by facilitating interaction with old friends, sharing of events, distribution of data and various other aspects of social life. Mobile based social networks like GyPSii, Brightkite, Loopt provide some exclusive features like short messaging notification, maps and location based services etc. Indeed, most of the popular social networking websites are transforming into mobile domain by offering exciting applications and games exclusively designed for users on the go. However, current social networking applications are rather streamlined. Furthermore, the major goal seems to be to get as many users as possible within the network and this is also the major figure used by analytics firms [1]. Whether the existing online social networks would be able to sustain continuing popularity is a highly debatable issue but there is an agreement in broader sense that the current open trend would be shifted towards closed user groups in the coming decade [2].

In this paper, we focus on these so called closed social network groups. In a closed group, there is no need to ”find anybody” in the country or the world in the network, but the important thing is to attract high end smart phone users by offering small and ”closed” dedicated existing network. The groups can be created, modified or deleted by the users targeting specific community having common interest in short or long term. Hence, the groups would have restricted membership along with role based security set by moderator of that specific group. The closed community could be anything from an enterprise project team to a religious community or the like. As compared to typical social networks, we have high security requirements for the schemes used to identify and communicate between members within a group as well as between members from different groups. Typically, the security offered at most social networking sites is simple login protection based on usernames and passwords and users are forced to remember login credentials or to write them down. Moreover there is a common tendency among users to store private and sensitive data on their mobile phones as compared to typical personal computer like contacts, passwords, bank account details, updated calendar entries with key dates and personal notes. Hence for mobile based social groups, there is a need for user friendly as well as more secure methods to enrol new members into the group.

Mobile based communications are considered to be fairly safe and trusted by end-users and most mobile units already provide strong authentication through the USIM/SIM or ISIM module. Thus, it would be efficient to utilize the existing authentication possibilities provided by these modules and corresponding standards while designing solutions for strong authentication in close environments. The security design provided in this paper is an effort to probe and improve the existing key-exchange mechanisms for USIM, ISIM environments to provide secure identification in mobile social networks. The main contributions of the parer are the following:

- We provide a secure identification architecture based on

[1]This paper is part of the Research and Development project carried out at Swedish Institute of Computer Science ’SICS’ in collaboration with Sony Ericsson AB.

the 3rd Generation Partnership Project (3GPP) Generic Bootstrapping Architecture (GBA) [3] that can be used to securely enroll members to a closed mobile social group or to identify members in the group. Our architecture is based on the assumption of the existence of a Mobile Social Networking Portal (MSNP) responsible for enrolling online members.
- We provide a new user friendly scheme, compatible with the suggested identification architecture for securely enrolling member within close proximity using short range wireless technologies.
- We have made a prototype implementation in order to verify the proposed security architecture and schemes.

This paper is organized as follows. Section II describes the fashion industry use case and state of the art. Some notations and design limitations are discussed in Section III. Section IV provides our secure identification design with different scenarios. Section V discusses the prototype implementation for this paper followed by discussions on its security analysis in Section VI. Finally, we conclude in Section VII.

II. Preliminary

In order to illustrate the security challenges addressed within this paper, we discuss a social networking use case related to closed environment below. We use this use case to identify security requirements and usability aspects that should be taken into account for the secure architecture design. Moreover, we give and overview of the 3GPP Generic Authentication Architecture (GAA) [4]. Finally, we discuss device pairing protocols and their applicability with respect to creating initial social network security association utilizing physical proximity between peers.

A. A Fashion Industry Use-case

We consider a modeling company having staff comprising of managers, marketing personals, dress designers, choreographers, beauticians, photographers, models, office staff, etc. The company works in close co-operation with certain media groups and enterprises for marketing their products and arranges various events and fashion shows funded by enterprises. The company would certainly benefit by having a closed mobile based social network, i.e. comprising of only directly invited members after strong authentication, which can become the backbone for its operations at fashion events. The prime focus of the event manager is to make sure that every person involved in the event organization should be aware of its tasks both prior to the event and during the event. The portal will help the event manager to announce the description of event, status and availability of models, post event discussions, etc. The prime interests related to the services offered to these groups could be:

- Event Announcements and Schedule Updates
- Calendar Sharing
- Location Based Services
- Shows Details (Ramp Numbering etc.)
- Document Sharing
- Media Sharing
- Post event Comments

The event manager should be able to create a temporary de-centralized user group where he/she can send invitations to other users involved in the event. One of the important factors is the fact that only those invited users should be able to register without any chance of fabrication. Some users of this group would also be reluctant to reveal their location so that they should be assured of anonymity protection. Another challenge would be to provide temporary access to some personals for any specific event, i.e. company wants to hire a beautician overseas for some particular event held in that country or city. Hence various user profiles should be maintained, and security levels for these profiles should not be compromised.

1) Business analysis-fashion industry: There is a substantial drift between the requirements of the mobile based use-case presented above and traditional online alternatives for these types of requirements. There is not any famous online social network dedicated for the requirements of the fashion industry, and most of the media companies have to depend heavily on human-resource departments or individual personal to manage the majority of the fashion events, including photo shots, media interactions, etc. The public figures from the fashion industry also have to compromise between two extremes of using traditional public social networks or interacting privately with their colleagues, family or friends. Moreover, celebrities have a tendency of being tentative to reveal their identity to unknown online users. Finally, the requirements discussed in our use case can't be managed by any online social network like location tracking, privacy protection, authentication forwarding, direct mode, etc.

2) Technological aspect: The use case poses a challenge for existing security, media sharing, content distribution standards and bringing these technologies together for realizing mobile social networks. It requires a networking online portal that is accessible by mobile units. It is evident that membership is restrictive as compared to traditional online social networks. Hence the portal must provide strong security guaranteeing that:

- Only invited members can join the network after strong identification and verification mechanism. If registration is triggered by some other member in direct offline mode, then secure identification and authentication procedures for device pairing should be implemented.
- There must be a strong authentication mechanism for user verification. Moreover, in case of identity service, the overall system delay must remain under some well-defined threshold limits.
- All communication between portal, fix or mobile terminals should be protected using confidentiality and integrity protection mechanisms.
- Content storage and distribution mechanisms should be applied to prevent information leakage.
- User privacy must be ensured such that it should not be possible for the non-group members to identify any

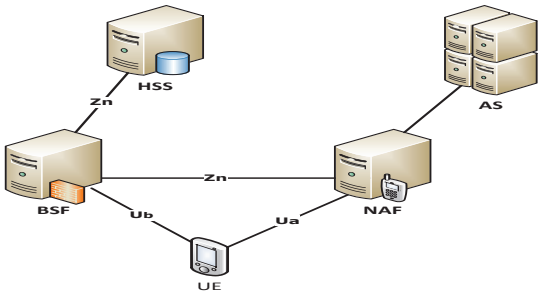

Figure 1. Generic Bootstrapping Architecture

particular group members or their locations. Furthermore, there should not be any possibility for non-group members to identify that a certain communication exchange is performed with a particular group or some specific users within that group.

- Fine grain access control should be supported to allow easy management of user roles and prevent illegal access to services and information within groups.

B. Generic Bootstrap Architecture

GBA has been specified by 3GPP for providing secure bootstrapping functionality between user equipment, mobile network operators and various application servers. The main advantage of the scheme is to reduce the client effort for managing multiple authentication profiles for different types of mobile applications along with improved levels of security. The old standard that uses mobile equipment to store authentication details was referred as GBA_ME, while the new GBA_U standard stores these credentials on the Subscriber Identity Module (SIM) or what is referred as USIM in 3G/4G networks. Although there are lots of changes among the old and new standard but backward compatibility is ensured. GBA do not provide single sign-on service like OpenID but the basic idea is to securely authenticate mobile users for various application servers by using pre-shared security information among Mobile Network Operators (MNO) and the end-users. GBA relies on 3GPP Authentication and Key Agreement Protocol (AKA) to authenticate peers and to agree on session keys between clients and application servers. There are five entities that are involved in the GBA authentication as shown in Fig. 1.

- **UE** (User Equipment): The client handset.
- **BSF**(Bootstrapping Server Function): The BSF is responsible for communicating with UE from the network side. The UE performs authentication with BSF maintained by MNO. The UE and BSF mutually authenticate each other using the AKA protocol.
- **NAF**(Network Application Function): The NAF is the application interface towards the UE. The NAF can be an internal application service maintained by the MNO or any external application of choice. In later case, the NAF must communicate with the BSF using a Zn-Proxy over the Zn interface. The Zn-proxy is not required if both BSF and NAF are on the mutually trusted MNO network.
- **HSS** (Home Subscriber System): The HSS stores the authentication profiles of users for applications known as User Security Settings (USS) [3]. The NAF fetches these profiles via BSF.

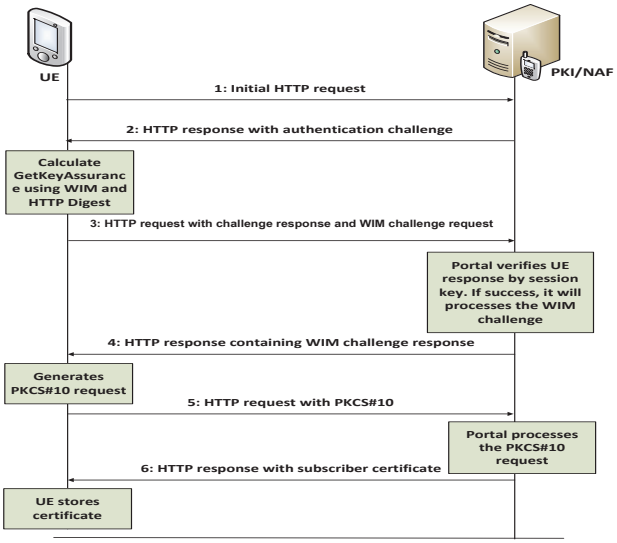

Figure 2. Message flow for issuing certificate [5]

C. GAA and Issuing of Subscriber Certificates

GBA is a part of the GAA architecture [4]. The GAA architecture supports two different types of authentication mechanisms, symmetric and asymmetric. Symmetric authentication is achieved through the GBA schemes we already discussed above and asymmetric authentication through usage of so-called subscriber certificates (SSC) [5]. Subscriber certificates according to GAA are issued in a two steps process, where the first step is a bootstrapping step using GBA where the requesting client, and the NAF derive a shared secret. This secret is in turn used in the certificate issuing process. The message flow for subscriber certificate issuance (from a PKI portal taking the NAF role) is illustrated in Fig. 2 and the different steps are the following:

1) The UE sends an empty HTTP request for a certificate to the NAF over the Ua interface.
2) The PKI portal/NAF sends an authentication challenge to the UE.
3) The UE uses its session keys obtained during the GBA process from BSF and use this secret to send a challenge response to the PKI portal. Optionally the UE also sends a so-called Wireless Integrity Module (WIM) [6] challenge to the PKI portal.
4) The PKI portal verifies the UE response, and if it is OK, it sends an acknowledgement message to the UE optionally also containing a WIM response (if a WIM challenge was received in the previous step).
5) The client sends a PKCS#10 [7] based digested request for issuance of a new certificate.

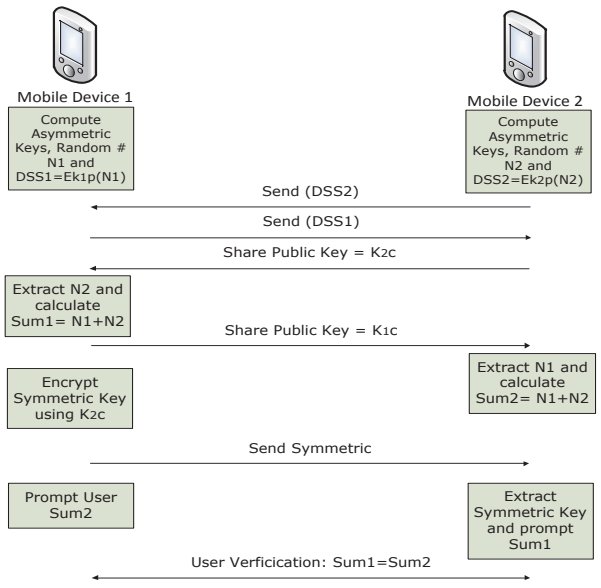

Figure 3. Device pairing using ViDPSec [9]

6) The PKI responds by returning an integrity protected client certificate. The client stores the obtained certificate either on the mobile equipment memory (GBA_ME) or in the USIM (GBA_U).

D. Device Pairing Protocols

Device pairing over an insecure wireless channel without the aid of any external link or mutually trusted 3rd party relies heavily on strong key management and authentication procedures. The notable solutions for such problems are suggested by Manual Authentication for Wireless Devices (MANA) family of protocols. The solutions can be categorized as: 'using data output of one device as input of 2nd device, comparing output of both devices and entering same data into both devices' [8]. These solutions can provide basic foundation for secure authentication of two devices in offline mode and can be easily modified for exchange of certificates and other services.

One example of a MANA protocol is the Visual Device Pairing Security Protocol (ViDPSec) [9]. The protocol is used to establish a shared key between two devices using asymmetric crypto system's key exchange mechanism. The message exchanges in the ViDPSec are shown in Fig. 3. Both parties calculate asymmetric key pair of public (Kc) and private (Kp) keys along with random numbers N1 and N2. The random numbers are signed using private key and shared among devices. In next step public keys are shared to read signed messages of previous step and both parties calculate sum of corresponding random numbers. The symmetric encryption key used for confidentiality for further session is shared in the next step and decrypted using the already available public key of the other user. Finally the user manually verifies the Sum on both devices to complete the authentication procedure [9].

III. Design assumptions and notations

We have based our architecture design upon a set of basic assumptions, which we list below:

1) The GBA network elements BSF, HSS etc. are assumed to be trusted by our design.
2) The security profile needed for bootstrapping is managed by the PKI portal over Zn interface or via a Zn-proxy in case of foreign network as per 3GPP GBA specification [3].
3) The MSNP acts as an Certification Authority (CA) and would extend the GBA based USS for issuing, delivering and revocation of certificates. This additional set of data gathered from the user including information related to certificates structure would be termed as MSNP based User Security Settings (MUSS). The MUSS is needed to specify the role of a specific user within various social groups.
4) The model does not include the format of managing certificate store at the PKI portal, trust hierarchy towards operator root certificate etc.

Fig. 4 illustrates the MSNP based secure identification architecture we propose and the notation (reusing the 3GPP GAA notations whenever applicable) we use to describe the architecture:

- *Ub Interface*: This interface is the primary communication channel between the UE and the BSF for agreement of session keys using the AKA protocol.
- *Ua interface*: The Ua interface represents the secure channel that is created as a result of a successful GBA bootstrap over the Ub interface.
- *Um interface*: This is the new interface that we introduce in the architecture, and it is the interface used for communication between the UE and the MSNP. It extends the security association over the Ua interface and support XML based encryption for identification, verification and registration of the users.
- *MSISDN*: Mobile subscriber unique identity number (cell phone number).

IV. Secure Identification Design

In this section, we describe our architecture for the secure group enrolment as well as authentication for mobile social network groups. The MSNP is the core component, but it only acts as a central "registration authority" and the solution allows as well enrolment and authentication between group members when no connection to MSNP is available. The solution comprises an extension of GBA based authentication along with offline authentication and key exchange mechanisms in compliance with GAA specification. We have chosen the certificate based mechanism for performing secure identification and authentication of a user due to its flexibility.

A. Architecture Overview

Fig. 4 shows the network model for GAA infrastructure for bootstrapping, certification and its extension to support

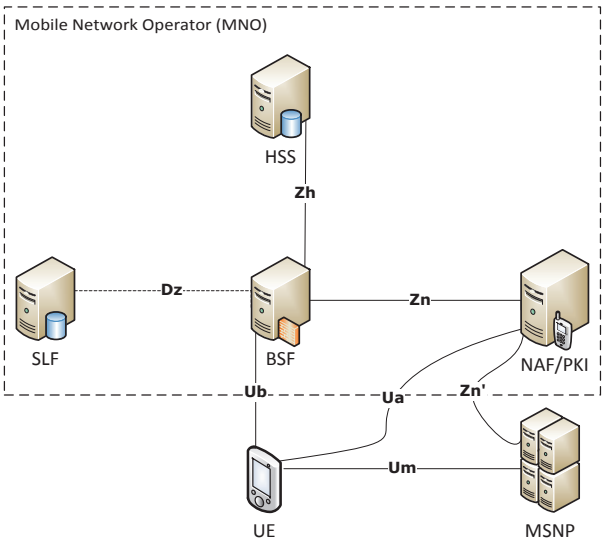

Figure 4. Architectural model for MSNP

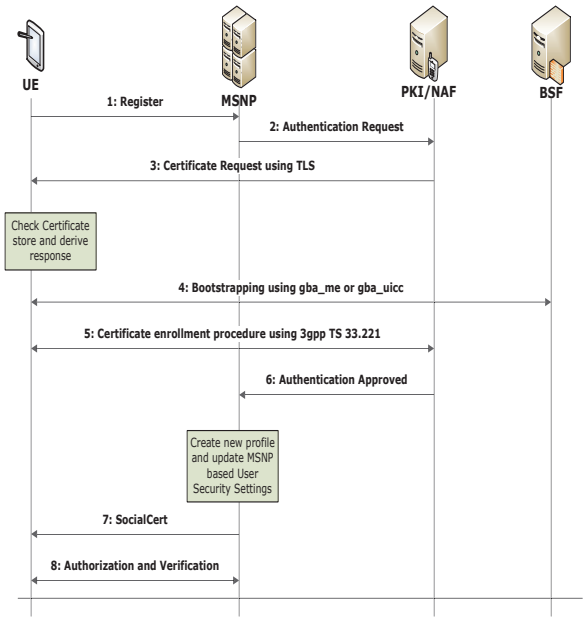

Figure 5. Registration flow for new user

MSNP. The solution is based on public/private key pairs and corresponding certificate signed by the PKI portal managed by MNO. The solution is built upon the following networking elements:

- The bootstrapping procedure and agreement on session keys to be utilized by the MSNP are managed using standard GBA bootstrapping procedures as defined in 3GPP GBA specification. The PKI portal will manage certificates as mentioned in 3GPP SSC specification based on USS and an extension for secure mapping using local profile information obtained from MSNP.
- The certificates are issued using X.509 version 3 extended certificate format as mentioned in RFC 3280 [10].

B. User Certificate Enrolment

The MSNP will issue three certificates for identification, verification and maintaining status profile within each social group. The basic requirements and the type of certificates issued to manage these demands within the solution can be summarized as:

- Every MSNP user will be issued one identity certificate for secure identification. Let us call this AuthCert_A, AuthCert_B etc. (for user A, B).
- The user should be able to verify different service requests etc. To ensure this, every user will be issued a signing certificate, SignCert_A, SignCert_B etc. (for user A, B).
- The MSNP registered user and holder of identity and signing certificates can be a part of more than one social network. Moreover the user might have different roles within different networks and these roles may change over time. So each user also has an additional certificate for verification of his/her membership and specific role in different groups. This certificate includes all groups that the particular user is a member of and the status of the group. This certificate will be referred as SocialCert_A, SocialCert_B etc. (for user A, B). The SocialCert must also contain pointers (One-way hash over the complete certificate or just the public key) to the AuthCert and SignCert. To enhance the privacy in offline authentication mode, the user can also maintain separate SocialCert for each group he/she is a member off.

C. New registration and the creation of a new social group

Next, we describe our proposed procedure for the creation of a new social group. The procedure is illustrated in Fig. 5 and can be summarized as:

1) The UE will start a secure TLS session with the client using an installed browser plug-in or a client application. MSISDN should be used as client id for initiation of secure identification procedure.
2) The MSNP will verify the identity of the UE to establish that it is a new user or an existing MSNP user. In case of a new user, it will forward the UE request for registration along with MSISDN to the local PKI/NAF for verification of authenticity. The PKI portal will then send a certificate request message to the UE.
3) The UE will check the supported certificate list mentioned in certificate request message and reply with an empty response (UE can reply with operator AuthCert if it already holds such certificate in its certificate store). The PKI/NAF will then initiate a bootstrapping procedure and request the UE to start a GBA based authentication procedure. Next, the UE and BSF will mutually authenticate each other over Ub interface and derive session keys using AKA protocol as mentioned in 3GPP TS 33.220 [3].

4) The UE will respond to the PKI/NAF with the B-TID obtained via the GBA process in the previous step. The BSF will validate this B-TID with the BSF over Zn interface (via the Zn proxy in case of foreign network) as mentioned in 3GPP TS 33.220.
5) If the client is authenticated, then the client will be issued new authentication and signing certificates signed by the PKI portal according to the 3GPP TS 33.221 [5] specification using X.509 certificate structure.
6) The PKI/NAF will update the MSNP application over the Zn interface and the user registration process will be completed. Furthermore, the user will be able to create a new social group with an active status. In this case, a new social network with unique name/ID is created and the MUSS is updated with the MSISDN of the UE, which will take the moderator role of the newly created social network group.
7) The MSNP generates the SocialCert and sends it over Um interface to the user.
8) The MSNP will securely interact with the UE to allow the user to use that social network group.

D. Secure authentication of registered users

The registered users of the MSNP already contain unique MSISDN for the MSNP and are holders of authentication and signing certificates. The users that are member of any social group would have an additional social certificate stored in their equipment or USIM using the procedure described in the previous section. The users should be able to:

- Perform mutual authentication with MSNP using AuthCert issued by the PKI using TLS handshake.
- Access services of those social groups that he/she is already member off by using the SocialCert after establishment of secure connection with MSNP.

E. Online invitation to new members

The suggested procedure for online invitation of new members is shown in Fig. 6 and it can be summarized as:

1) The moderator performs mutual authentication with MSNP using the authentication certificate (AuthCert) issued by the PKI over an HTTPS connection.
2) The moderator has the group access through the social certificate of the group that he/she moderates. The moderator of the group can either explicitly invite new members using MSISDN or by searching the interface provided by the MSNP. The entry of invited user will be updated in the database.

A similar request of any registered but un-authorized user (not moderator of that specific social group) will be marked as invalid by the MSNP after validating Role_ID with Group_ID using MUSS.

F. Joining procedure for user invited in online mode

The moderator of one social network is entitled to allow new users to enter a group and create their appropriate profile which may vary from group to group depending on the settings

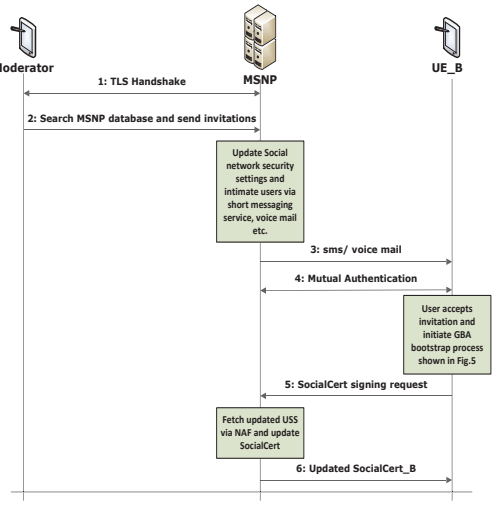

Figure 6. Online invitation flow initiated by moderator

and applications support in each group. The procedure used by the MSNP to authenticate an already registered client, says 'B', is shown in the steps 4-6 of Fig. 6 and can be summarized as:

1) The invited user authenticates itself using AuthCert_B.
2) The MSNP will validate the client and the request will be mapped by the database to confirm invitation status by the moderator and valid lifetime of that particular request.
3) The client will be routed to perform GBA based authentication as shown in Fig. 5 to generate new keys and update its SocialCert_B.
4) The user will generate the certificate signing request using updated keys and send it to the MSNP.
5) The MSNP updates the SocialCert of the client and includes the membership of that particular group.

G. New group creation by already registered members

The registered users of MSNP can:

- Securely perform mutual authentication using AuthCert issued by PKI over the HTTPS connection.
- The users (regardless moderator or member) of one group can opt to create a new group by following the procedure mentioned in Fig. 5. The user and PKI should re-negotiate cryptographic keys using GBA to mutually authenticate each other and fetch session keys for updating the SocialCert.
- The MUSS for a specific group is updated and the client will store the updated social certificate on its UE or USIM.

H. Secure Identification in offline mode

With respect to direct offline communication between MSNP clients, we consider the following two situations:

- Both parties are registered users of the MSNP and hold authentication certificates. One of the two users is a

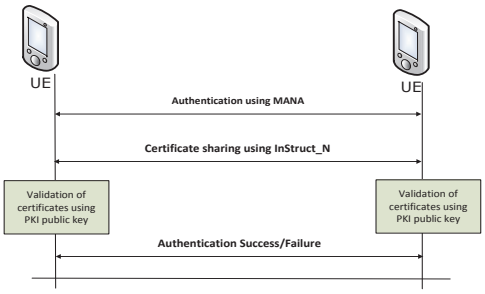

Figure 7. Offline authentication procedure for non-registered users of particular group

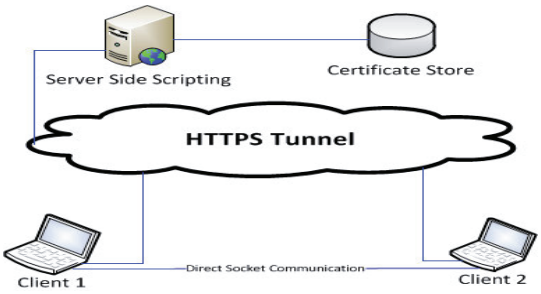

Figure 8. Prototype Architecture

moderator of some social group and willing to invite the other user to join his/her closed group in the offline mode.
- In this case, both users have been already registered to the same group and want to mutually authenticate each other in the offline mode using a client application.

1) Offline invitation by a moderator: The authentication flow for inviting a new member to MSNP and client enrollment in MSNP database is depicted in Fig. 7. Suppose user A, who is a moderator of group N want to invite user B who is the registered user of MSNP for another social network group. The steps in this procedure can be summarized as:

- Both parties (A and B) will perform mutual authentication as shown in Fig. 7 using any device pairing protocol along with AuthCertA and AuthCertB respectively.
- The user A will sign a special-purpose XML (or any other compatible format) encoded invitation structure say 'InStruct_N', using the SignCert_A. The user A sends the complete invitation encrypted by MSNP public key containing:
  1) ID of group N
  2) Role_ID (Assigned role of user within the group N)
  3) Nonce (Time Stamp)
  4) SignCert_A

The user B should have online communication with MSNP prior to its communication with other members of the invited social network group for successful completion of the registration process and obtain its updated SocialCert_B from the network operator of MSNP. Whenever the user B goes online, it authenticates itself with MSNP (using AuthCert_B) and present InStruct_N for verification. The MSNP will push user B for GBA bootstrap procedure as defined in 3GPP 33.223 [11] specification. Next, the PKI portal will complete the GBA bootstrapping procedure with the BSF over Ub interface and perform mutual authentication using the Zn or the Zn-proxy interface. The user is added to the social network N with the role defined by inviting user, and the social certificate of user B (Social- Cert B) is updated to include membership in the group N.

2) Offline authentication of users belonging to same group: The users who are already registered to the same mobile social network within MSNP can authenticate each other by the following procedure:

- Both parties will perform initial authentication using corresponding MSNP authentication certificates.
- The users will then use social certificates for verification and offline connectivity as they are part of one social group. The social certificate of each user will also determine its corresponding role within the group.

V. Prototype Implementation

This section briefly describes the prototype implementation that we have done using the solution discussed in the previous section. The software and hardware requirements can be categorized as:

- *Application Language*: HTML, CSS, PHP 5.3
- *Operating System*: Windows, Linux
- *Protocols*: HTTPS (SSL)
- *Web Server*: Apache (2.2.11)
- *Database*: MySQL

All the cryptographic keys and Certificates Signing Requests (CSR's) are generated at client side. The prototype server on the other hand is creating all the corresponding certificates, database storage etc. Following hardware is used for the smooth execution of prototype especially at the client end while using 2048 bit RSA keys:

- X86 based core i5 Processor
- 4GB of RAM
- 500 MB of free space on storage media

A. Platform and Requirements

The prototype architecture is shown in the Fig. 8. The web based prototype functionality is primarily based upon two software modules (API's) supported by PHP [12].

- OpenSSL module of the PHP uses OpenSSL functions for creation of x.509 certificates, confidentiality and integrity of data. The key pair generation, CSR's, X.509 based certificates, data encryption, decryption, hashing and SSL based communication tunnel is supported by using various functions of this API.
- The PHP socket extension is primarily based on the most widely implemented BSD sockets interface. The Transmission Control Protocol (TCP) was chosen for the client/server communication in offline mode due to its reliability.

VI. Discussions

Next we discuss our solution and in particular, our prototype implementation and analyze the solutions from an information security perspective. The security of solution primarily depends on access control mechanisms to guard keys and certificate storage both at the client and the server. The complete connection setup and subsequent sessions are strongly authenticated, and the communication is carried out in secure tunnel using SSL. The secure connectivity covers:

1) User authentication in online mode
2) Server authentication by corresponding certificates
3) Access authentication in offline mode using ViDPSec

A. Security Analysis

Our proposed architecture utilizes well established 3GPP standards for the enrolment of users to the MSNP as well as for the issuing of group certificates. Hence, the risks of compromised protocols or networked based attacks are low. However, this is only true as long as the client implementation also applies careful end user authentication, and platform based credentials for access control mechanisms. The design and implementation of such a mechanism are outside the scope of the current paper. The security of the MSNP depends on its deployment and necessary means for protecting it from both the network based and direct physical attacks.

The security of the off line invitation is dependent upon the ViDPSec security. However, alternative MANA protocols can be used and still be compatible with our suggested architecture. Furthermore, the ViDPSec protocol can be replaced with a very close proximity wireless communication interface such as NFC, in which case the risks of direct wireless attacks are low and there is much less need for manual authentication of the group invitation communication.

VII. Conclusion

In this paper, we have investigated the security issues with respect to the design of a secure identification infrastructure for so call closed social groups. Selecting a concrete use case as the starting point, we have identified the most important security requirements for such scenario's and conclude that these are indeed different from what one expects from the widely used open social groups. Based on these requirements, we have defined a secure identification architecture based on the 3GPP GAA architecture. This architecture allows mobile users equipped with USIM to securely enroll, create and manage social groups through an MSNP portal function in the mobile operator network. In addition, we have investigated how to align general online group management with offline group invitation and authentication. This will allow quick, secure and user convenient invitation to new group members through interaction with users who are close by. The basic mechanisms and protocols have been implemented in a prototype system depicting the feasibility of the proposed design. The suggested architecture shows the power of the GAA standard framework in a social network context. The work also shows how basic security (confidentiality, access control and integrity) can be achieved while additional important security aspects such as end user privacy have been left for the future research.

References

[1] "History of social networking websites." [Online]. Available: http://www.articlesbase.com/internet-articles/history-of-social-networking-websites-1908457.html [Accessed: 2012-11-21]

[2] "Social wireless networks, secure identification (swin project)." [Online]. Available: http://www.sics.se/projects/swin/ [Accessed: 2011-08-17]

[3] *Generic Bootstrapping Architecture (GBA)*, Technical Specification Group Services and System Aspects; (3G Security), 3rd Generation Partnership Project; 3GPP TS 33.220, ver 9.3.0, June 2010.

[4] *Generic Authentication Architecture (GAA)*, Technical Specification Group Services and System Aspects; (3G Security), 3rd Generation Partnership Project; System description; 3GPP TR 33.919, ver 9.1.0, June 2010.

[5] *Support for subscriber certificates (SSC)*, Technical Specification Group Services and System Aspects; (3G Security), 3rd Generation Partnership Project; 3GPP TS 33.221, ver 9.1.0, June 2010.

[6] *Wireless Identity Module (WIM)*, OMA Security Part: Security ver 1.2, 2005.

[7] "PKCS#10," Certification Request Syntax Standard. [Online]. Available: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf [Accessed: 2011-10-10]

[8] C. Gehrmann, C. Mitchell, and K. Nyberg, "Manual authentication for wireless devices," *RSA Cryptobytes*, vol. 7, no. 1, pp. 29–37, 2004.

[9] D. Zisiadis, S. Kopsidas, and L. Tassiulas, "Vidpsec visual device pairing security protocol," in *International Conference on Computational Science and Engineering*, vol. 3, TKK T-110.5290, 2009, pp. 359–364.

[10] W. F. R. Housley, W. Polk and D. Solo, "RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," IETF, Tech. Rep., April 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3280.txt [Accessed: 2011-10-17]

[11] *Generic Bootstrapping Architecture (GBA) Push function*, Technical Specification Group Services and System Aspects, 3rd Generation Partnership Project; 3GPP TS 33.223, ver 10.0.0, March 2011.

[12] "PHP: OpenSSL - manual." [Online]. Available: http://se.php.net/manual/en/book.openssl.php [Accessed: 2011-11-08]